UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF WISCONSIN

In re: Two email accounts stored at Google, Inc.

Case No. 17-M-1235

ORDER

I. Introduction

In 1986, spurred by concerns that the then-current law was "hopelessly out of date," S. REP. 99-541, 2, 1986 U.S.C.C.A.N. 3555, 3556, Congress amended the Omnibus Crime Control and Safe Streets Act of 1968 with the Electronic Communications Privacy Act. PL 99–508 (HR 4952), PL 99–508, October 21, 1986, 100 Stat 1848. Included in the Act was the Stored Communications Act (SCA). At the time the SCA was enacted, the internet did not exist in any practical sense and email was in its infancy. *See* S. REP. 99-541, 8, 1986 U.S.C.C.A.N. 3555, 3562, 3563-65 (describing remote computer services, "computer-to-computer communications" and "electronic mail"). Yet this decades-old statute, with a few intervening amendments, remains the primary tool used by law enforcement to access a myriad of electronic communications and records.

Naturally, many aspects of contemporary technology are not directly addressed in the antiquated law. As technology continues to change beyond bounds even

imagined three decades ago, prosecutors and law enforcement are more and more asking courts to proverbially fit square pegs into round holes – trying to make current technology fit within the outmoded constructs created by Congress in 1986 – such that the law might again be called "hopelessly out of date." But it is not the court's role to strain the strictures of a statute to create a space to fit each request from the government. If the court concludes that the government's request is outside the bounds of the statute, the court is obligated to reject it. That is true regardless of how practical or logical the request might seem; if there is a gap in the law, it is the obligation of Congress, not the courts, to fill it.

According to Google, Inc., the present case implicates one such gap in the law. On February 15, 2017, the government asked the court to issue a warrant commanding Google to disclose email records associated with two particular Gmail addresses. Google has turned over responsive records that it concluded were stored in a data center in the United States. But a dispute exists as to records that are or may be (for Google sometimes cannot be certain where a record is) stored in a data center outside the United States. Google's position is that this court's warrant may not reach property stored outside the United States.

In light of the recent decision by the Court of Appeals for the Second Circuit in the case of *In Re: Matter of Warrant to Search a Certain E–Mail Account Controlled & Maintained by Microsoft Corp.*, 829 F.3d 197 (2d Cir. 2016), when issuing the present

warrant the court *sua sponte* paused to consider whether it can order Google to disclose information that Google stores on servers located outside of the United States. The court concluded that such an order was authorized under the SCA and issued a Memorandum in conjunction with the warrant. *See In re Info. Associated with One Yahoo Email Address that is Stored at Premises Controlled by Yahoo*, 2017 U.S. Dist. LEXIS 24591 (E.D. Wis. Feb. 21, 2017) (discussing the present warrant along with a separate contemporaneous application regarding a Yahoo email address). Google has moved to "amend" the warrant to exclude any data that it stores on servers located outside the United States. (ECF No. 8.) The court now considers its prior order anew with the benefit of adversarial argument and a more thorough record.

II. Relevant Facts

Because the facts presented in the application relate to an ongoing criminal investigation and an unexecuted warrant, they will be addressed here in only the broadest terms. For present purposes it is sufficient to state that the warrant relates to the investigation of persons who have already been indicted in this district. There is no indication that the relevant email accounts were used by persons outside the United States.

The parties stipulated to various other facts relevant to the present motion. (ECF No. 11.) Google is headquartered in California. (ECF No. 11, ¶ 1.) It stores user data at various locations, some of which are in the United States, some of which are not. (ECF

No. 11, ¶ 2.) A user's files might be broken into component parts, and different parts of a single file may be stored in different locations, including in different countries. (ECF No. 11, ¶ 3.) Google automatically moves user data to optimize performance, reliability, and other efficiencies. (ECF No. 11, ¶ 4.) Thus, data might be stored in one location when the government seeks a warrant and in a different location by the time Google is served with that warrant. (ECF No. 11, ¶ 4.) If data is stored in a foreign country, the tool that Google uses to identify data responsive to the warrant does not identify which specific foreign country the data is stored in. (ECF No. 11, ¶ 4.) The only Google personnel who can access data in response to a warrant are located in the United States. (ECF No. 11, ¶ 5.)

III. Relevant Law

The government may obtain a warrant requiring "disclosure by a provider of electronic communication service of the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system." 18 U.S.C. § 2703(a). Translated into simplified terms relevant to the present case, this means that a federal law enforcement officer can ask a United States Magistrate Judge to issue a warrant compelling an email service provider (e.g., Google, Yahoo, Microsoft, etc.) to disclose emails associated with a particular email address. (Again, the statute covers other sorts of information and the relevant application seeks details other than emails, such as account information, but for the sake of simplicity the court will refer here to

emails.) If the law enforcement officer demonstrates that probable cause exists to believe that the emails will contain evidence of a crime, the court will order the email service provider to disclose the emails sent from or received at the identified email address.

With respect to search warrants generally, under certain circumstances a magistrate judge may issue a warrant authorizing a search in a district other than his or her assigned district. Fed. R. Crim. P. 41(b)(2)-(6). However, aside from narrow exceptions related to searches in a "territory, possession, or commonwealth" of the United States, and properties associated with consular missions, Fed. R. Crim. P. 41(b)(5), Rule 41 is silent as to whether a federal court may issue a warrant for the search of property located outside of the United States.

IV. Analysis

According to Google, a warrant issued under 18 U.S.C. § 2703 is analogous to the court authorizing a government agent to enter a location in a foreign country, open a file cabinet, and seize all the papers it contains. Because it is presumed that a federal court does not have statutory authority beyond the United States, the court's order authorizing the seizure of data located in a foreign country was an impermissible extraterritorial order. The government views the warrant as more akin to a court order directing a person in the United States to collect records under that person's control and provide them to a government investigator.

Google rests its position largely on two contentions. First, it argues that the relevant provisions of 2703 use the term "warrant," which traditionally means an order regarding the search or seizure of physical property rather than an order compelling action by a person. Second, it contends that under the SCA Congress recognized emails as belonging to the user. If the warrant relates to the seizure of an object, albeit a digital "object," the location of that object is material. If that object is stored on a server located outside the United States, any warrant authorizing its seizure implicates extraterritoriality considerations.

The government characterizes the distinction between a traditional search warrant and a § 2703 warrant as one of *in rem* versus *in personam* jurisdiction – whether the court is authorizing the government to search for and seize certain property or whether the court is ordering a person to do something. In the government's view, a 2703 warrant compels action by a service provider (e.g., Google), and thus what matters most is whether the service provider who will disclose the data is within the reach of the court.

The Court of Appeals for the Second Circuit took Google's side in the debate, concluding that if the records are stored in data centers located outside the United States they are outside the reach of a United States court. *Matter of Warrant to Search a Certain E–Mail Account Controlled & Maintained by Microsoft Corp.*, 829 F.3d 197 (2d Cir. 2016). However, to date, the Second Circuit has been the only court to take this side. All

courts outside the Second Circuit that have considered the issue, as well as four judges of the Second Circuit who wrote in dissent of the court's decision not to rehear the panel's decision en banc and the magistrate judge and district judge who considered *Microsoft* in the district court, have disagreed. *Microsoft Corp. v. United States (In re Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp.)*, 2017 U.S. App. LEXIS 1274, 18 (2d Cir. Jan. 24, 2017); *In the Matter of Search of Information Associated with [redacted]@gmail.com*, 2017 U.S. Dist. LEXIS 92601 (D.D.C. June 2, 2017); *In re Search of Content that is Stored at Premises Controlled by Google*, 2017 U.S. Dist. LEXIS 59990 (N.D. Cal. Apr. 19, 2017); *In re Search Warrant No. 16-960-M-01*, 2017 U.S. Dist. LEXIS 15232 (E.D. Pa. Feb. 3, 2017); *In re Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp.*, 2014 U.S. Dist. LEXIS 133901 (S.D.N.Y. Aug. 29, 2014); *In re A Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp.*, 15 F. Supp. 3d 466 (S.D.N.Y. Apr. 25, 2014); *see also In re Search of Premises Located at [redacted]@yahoo.com, stored at premises owned, maintained, controlled, or operated by Yahoo, Inc.*, No. 6:17-mj-1238 (M.D. Fla., April 7, 2017) (available in the record as ECF No. 12-1) (reversing *In re Search of Premises Located at xxxxxxxxxxxxxxxxx@yahoo.com, stored at premises owned, maintained, controlled, or operated by Yahoo, Inc.*, No. 6:17-mj-1238 (M.D. Fla., March 21, 2017) (available in record as ECF No. 9-1)).

Having considered Google's arguments and the additional facts now before the court, the court again concludes that an emphasis on where the relevant data is located

at a given point in time is misplaced. "The data does not occupy any physical space, and it can be divided up and distributed anywhere." Orin S. Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 Stan. L. Rev. 1005, 1014 (2010). "Electronic 'documents' are literally intangible: when we say they are stored on a disk, we mean they are encoded on it as a pattern." *Matter of Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp.*, 855 F.3d 53, 61 (2d Cir. 2017) (Jacobs, J., dissenting from denial of rehearing). Thus, electronic data, especially data that exists within a free-flowing international information infrastructure, cannot be fairly equated to physical property. This is especially true with respect to data controlled by Google where Google's "state-of-the-art intelligent network … automatically moves data from one location on Google's network to another as frequently as needed to optimize for performance, reliability and other efficiencies." (ECF No. 11, ¶ 4.) In fact, the location of where data is stored at any given moment is so abstruse that even Google sometimes cannot determine whether the data is located inside the United States. (ECF No. 11, ¶ 4.)

The court agrees with the government that a § 2703 warrant is an order compelling action by a service provider, and the service provider, not the data, is the relevant subject that the court must reach for the order to be effective. Unlike a traditional search warrant, which commands law enforcement to do certain things, *see* Fed. R. Crim. P. 41(e)(2)(A), a warrant under 2703 compels action by a service provider.

For example, it states, "A governmental entity may require the disclosure by a provider of electronic communication service …," 18 U.S.C. § 2703(a), and "A governmental entity may require a provider of remote computing service to disclose …," 18 U.S.C. § 2703(b)(1); *see also* 18 U.S.C. § 2703(g) ("…requiring disclosure by a provider of electronic communications service …"). The terms "disclose" and "disclosure" are clearly directed toward the conduct of a service provider. Therefore, the court accepts the government's view that a § 2703 warrant is, in effect, an exercise of the court's *in personam* rather than *in rem* authority. Accordingly, the court finds that the concerns regarding extraterritoriality that were crucial in the court's analysis in *Microsoft* are not implicated here.

The court acknowledges that a customer has a privacy interest in the data and that through the SCA Congress sought to protect that privacy interest. But for purposes of the Fourth Amendment that privacy interest is protected by the fact that the government must obtain a warrant, supported by probable cause, from a magistrate judge before it may obtain the data. *See Microsoft Corp. v. United States (In re Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp.)*, 855 F.3d 53, 61 (2d Cir. 2017) (Jacobs, J., dissenting from denial of rehearing) ("Important as privacy is, it is in any event protected by the requirement of probable cause; so a statutory focus on privacy gets us no closer to knowing whether the warrant in question is enforceable.").

Moreover, that privacy interest applies to the content of the records; the court find no such privacy interest with respect to the location of the data. That is especially true in the present case, where Google freely relocates data to further its service needs and without affording the user any apparent control as to where the data is stored. Therefore, ordering a service provider to transfer data from a data center in a foreign country to a data center in the United States does not implicate the user's privacy interests or rights under the Fourth Amendment "because there is no meaningful interference with the account holder's possessory interest in the user data" as a result of the transfer. *In re Search Warrant No. 16-960-M-01*, 2017 U.S. Dist. LEXIS 15232 (E.D. Pa. Feb. 3, 2017).

V. Conclusion

In sum, the court finds that because the order is directed toward a service provider that is within the reach of this court the fortuity of where that service provider may store the relevant data at a given moment in time does not implicate extraterritoriality concerns. Nor does it implicate the user's privacy interests to order a service provider to transfer the relevant data to a data center in the United States so that it may then be turned over to the government pursuant to a warrant supported by probable cause. The search and seizure does not occur until the service provider discloses the demanded information to the government, and this occurs in the United States.

IT IS THEREFORE ORDERED that Google Inc.'s motion to amend the warrant (ECF No. 8) is **denied**.

Your attention is directed to 28 U.S.C. § 636(b)(1)(A), Fed. R. Civ. P. 72(a), and Fed. R. Crim. P. 59(a) whereby written objections to any order herein or part thereof may be filed within fourteen days of service of this order. Objections are to be filed in accordance with the Eastern District of Wisconsin's electronic case filing procedures. Failure to file a timely objection with the district court shall result in a waiver of a party's right to appeal.

Dated at Milwaukee, Wisconsin this 30th day of June, 2017.

WILLIAM E. DUFFIN
U.S. Magistrate Judge